White Paper – April 2021

SECURITY IMPLEMENTATION OF PRIVACY REGULATION

GOVERNANCE AND POLICY WORKING GROUP

Scott Franzitta- BSCI, Bob Haack- KARL STORZ Endoscopy, Elias Nyankojo-Avanos Medical
Viola Girgis- Johnson & Johnson, H-ISAC Oversight: Josh Singletary

H-ISAC™
HEALTH - ISAC

www.h-isac.org

SCOPE STATEMENT

This paper provides a recommendation for a minimum set of security controls and process tasks to protect Personal Identifiable Information (PII). In general, this paper addresses the intent of local and global privacy laws and regulations. The requirements to meet specific privacy laws or regulations should be clearly identified respective to that specific law or regulation.

PROCESS TASKS

A three-step approach is suggested for the application of Security Controls to Data Privacy protection:

1. **Selection of relevant controls**
2. **Implementation of relevant controls**
3. **Assessment and monitoring of relevant controls**

1. Selection of Relevant Controls

1.1. Identify unique privacy regulations for each country where the business is operating.

1.2. Identify the requirements that can be addressed via a security control application.

1.2.1. Classify the type of regulations into administrative, technical and physical control requirements.

1.3. Determine the systems that should take priority for implementation (i.e., crown jewel systems, systems that handle Sensitive PII, or systems in countries with the most restrictive Privacy regulations)

2. Implementation of Relevant Controls

2.1. Associate the requirements either individually or collectively, with an appropriate security control measure.

2.2. The control measure establishes a baseline set of security controls suited to address the regional and local privacy requirements.

2.3. Create processes and procedures for the implementation of the different types of security controls (i.e., administrative, technical and physical).

2.4. Leverage existing procedures towards the implementation of the security controls baseline before creating.

3. Assessment and Monitoring of Relevant Controls

3.1. Establish a security risk assessment process to verify the effectiveness of the baseline set of controls.

3.2. Establish a testing strategy to determine that the controls are implemented correctly and are operating as intended.

3.3. Establish a continuous review and monitoring process to account for changes to privacy laws and regulations and identifying additional security requirements.

Note: Security risk assessment evaluation of appropriate risk control relative to data privacy should still be measured against the three tenets of cyber security – **Confidentiality, Integrity and Availability**.

- **Confidentiality** ensures that privacy data is not available or disclosed to unauthorized persons or processes.
- **Integrity** ensures that privacy data cannot be altered or destroyed in an unauthorized manner.
- **Availability** ensures that privacy data is accessible and useable upon demand by an authorized person.

DATA PROTECTION:

ENCRYPTION

All sensitive information including data that can be tied to an individual through online identifiers such as username, email address, IP address, device configuration shall be protected during use. Protection can be facilitated by using encryption protocols. It is advised to avoid using weak encryption protocols, or previously deprecated algorithm. The NIST RMF FIPS 140-2 or ISO 27001 article 10 provide additional guidelines. The protection should extend to infrastructure, middleware, application as well as digital asset components.

The following protection methods requirement shall apply when non-business related Personally Identifiable data is stored electronically:

1 Protection at Rest

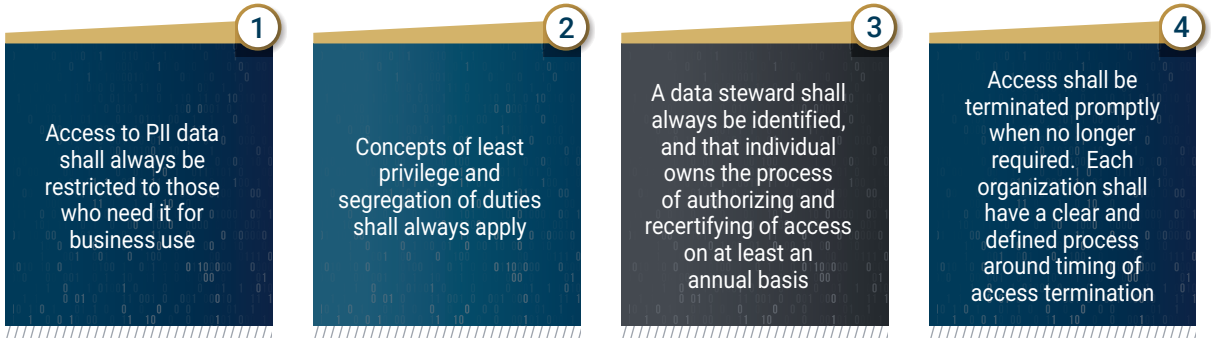
- Encrypted in a manner compliant with industry standard.
- Through appropriate physical protection to safeguard against loss, theft and unauthorized access.

2 Protection in Transit

- PII data shall always remain encrypted in transit using industry standards such as TLS 1.2 or higher cryptographic protocols.

ACCESS MANAGEMENT

The following are the guiding principles for access management to ensure data privacy for PII information.



AVAILABILITY

1. Defining requirements based on privacy system criticality to ensure minimum data availability is present:

1. Identify the systems that are considered critical to the business and would have the largest impact to the customers, products quality, company reputation, and/or employees' safety.

2. Depending on the type of PII data contained within the system, and the need for its continuous availability one of several of the following controls might be required. For example, systems containing PHI data used to treat patient might require higher availability than PII data that don't contain medical records.

1. Disaster Recovery is often expensive and may not be necessary for all systems. Identifying the systems that would have the greatest benefit from a disaster recovery program is the first step
2. When testing the DR, it is important to include Testing a table-top exercise in addition to the technical capability.
3. Business Continuity plan helps with assessing the reliance level on the technical solution. The BCP should inform the need for DR
4. Unlike disaster recovery, high availability can be performed at the same site where the infrastructure for the system is hosted. Since high availability can be more achievable, it should be an option for a broader range of systems containing less time sensitive data.
5. Data protection requirements should be maintained in the DR, HA environments same as production as long as production data is hosted in the environment.

SUBJECT RIGHTS

Establish the following process controls in order to assist with meeting Subject Rights regulatory requirements:

1. **An asset management program that can be** used to track all assets containing sensitive PII data
2. **A data categorization process** by which the data about the individual is categorized according to its purpose of collection and intended use.
3. **A data flow map that** shows flow of data across the network in order to recall it as necessary.
4. **Data access and control processes ensuring that** access to personally identifiable information is controlled as described in the access management section.
5. **Data Management Policy and procedures** that would outline how an organization would respond to inquiries related subject rights including but not limited to:
    - 5.1 Opt-in
    - 5.2 Opt-out
    - 5.3 Revocation
    - 5.4 Data removal and evidence of removal
    - 5.5 Record retention, legal requirements consideration (e.g., organization legal hold requirements conflict with request of subject data deletion.

LOGGING

Event logs shall record user and administrative activities, exceptions, errors, and security events.

LOG CONFIGURATION

Logs should be of adequate details to support events reconstruction. A group or individual directly responsible for the data or system must ensure logging is configured appropriately.

Some examples of what should be captured in log events include:

- Access attempts
- Successful and unsuccessful configuration of protection changes
- Privilege escalation
- Admin account usage
- Access to files or database records depending on security level
- Security alerts from applications, systems or account management
- Account creation, modification, deletion or change of privileges

Log entries should include at least the following:

- Event type
- User identifier
- Date/time
- Success or failure indicator
- Event origin
- System or service identifier
- Network addresses and protocols
- Use the ISO standard date and time format
- Ensure that clocks are all synchronized to the same source.

LOG ENTRIES PROTECTION

1. Log entries should be protected from unauthorized changes and operational errors
2. In order to ensure the integrity of the logs, separation of duties should be applied.
3. Best practices are to save log entries to a separate secure log server or off-site location via an one way process in the logs original format.
4. Logs should not be modifiable by the log generator.

LOG RETENTION

1. Define the baseline security controls for log retention based on the appropriate retention policy, applicable laws, or contractual agreements.
2. Any logs that are part of pending or current litigation may not be destroyed, regardless of existing record retention policy and schedule.
3. Logs should be securely disposed of once retention periods have been met.

LOG ANALYSIS

1. Define the baseline security controls for security log analysis, to include a threat prioritization map. A log analysis plan should also be documented and contain the roles and responsibilities of the different stages of analysis, schedule, process, documentation, tracking, and tools being used.
2. Log reviews should include the identification of anomalies, validation to remediations and mitigations applied.
3. Logging systems should be periodically tested to ensure any triggers or thresholds are properly functioning and not compromised.

INCIDENT REPORTING:

DATA PRIVACY BREACH INCIDENTS REPORTING

Key components to data privacy breach incidents reporting are:

1. Identification of data privacy breaching requirements that apply to your organization. Here there will be a need to build a global regulatory strategy that address complexity of different reporting statues
2. Breach notification guidelines and templates
3. Training simulation to breach incidents and reporting
4. Establishment of Breach Notification Plan
   - Data Privacy breach should be reported as soon as they are suspected and confirmed to allow investigation, remediation and reporting activities to begin immediately.
   - Organizations should establish procedures that define how they must prepare for and responses to a PII breach incident. This is can be referred to Breach Notification Plan. The Plan should provide responses and notification procedures ta different impact local, region and/or global areas.
   - Other organizations leverage third parties Data Breach Reporting services that allow the incident to be reported properly, to the correct regulatory bodies and consumers and within required time-frames. This mechanism could be part of the Breach Response Plan.

Feedback on this white paper and suggestions for future topics are encouraged and welcome. Please email us at contact@h-isac.org

www.h-isac.org